4 NOV 1981

MEMORANDUM FOR: Records Management Division
Office of Information Services

STAT FROM: [redacted]
Director of Security

SUBJECT: Revision of Executive Order 12065

1. I have reviewed the Information Security Oversight Office (ISOO) draft of the proposed Executive order to replace E.O. 12065, along with the ISOO comparison paper that purports to highlight significant change from previous Executive orders. My comments follow.

2. To my mind, the most significant change, which incidentally is not addressed in the ISOO comparison paper, is found in Section 4-201. The ISOO revision adds a provision that:

a. special access programs pertaining to cryptology may be created and continued only at the written direction of the Secretary of Defense, and

b. special access programs pertaining to intelligence sources and methods may be created and continued by the DCI.

The revision would permit COMINT to be considered as "pertaining to cryptology" and, in my view, would denigrate the authority of the DCI by removing him from a role in COMINT compartmentation. This interpretation is supported by deletion of the sentence, "For special access programs pertaining to intelligence activities (including special activities) or intelligence sources and methods, this function will be exercised by the Director of Central Intelligence, who shall ensure the establishment of common security, access, dissemination and control standards for such programs."

3. It would appear that the ISOO's revision of Section 4-201 is related to the addition in Section 1-301 of "cryptology" as a category of information that may be classified. ISOO states that the addition was intended to avoid jeopardy in the event of litigation and did not represent an effort to increase the range of material that may be classified under E.O. 12065. The expressed intent is valid, but it is not valid to use a partial

OS 1 0660/8

breakdown of intelligence sources and methods as supportive of diminution of the statutory responsibility of the DCI to protect intelligence sources and methods specified in the National Security Act of 1947.

4. The cited statutory responsibility of the DCI raises the point of possible conflict between existing law and the provisions of the ISOO draft. In effect, the ISOO approach divorces COMINT from intelligence sources and methods. The approach represents fallacious logic if the listing of "cryptology" in Section 1-301 is, as ISOO states, included in an existing category. If COMINT information does not qualify as the product of intelligence sources and methods, which of the other categories can accommodate it? I submit it is obvious COMINT cannot be considered as anything but an intelligence source and method and, therefore, cannot be divorced from the statutory responsibility of the DCI without a change in existing law. I strongly recommend that the Agency take the position that the language of Section 4-201 of the interagency working group's final revision of E.O. 12065 be retained.

5. Section 5-404 states that the Director/ISOO will be promptly notified whenever:

> a. Officers and employees of the U.S. Government "knowingly, willfully or negligently disclose without authorization information properly classified under this Order or predecessor orders," and
>
> b. "Knowingly and willfully classify or continue the classification of information in violation of this Order or any implementing directive."

There is no objection to the second reporting requirement. However, the Office of Security perceives a serious problem associated with the first. Many or most instances of unauthorized disclosure are developed during polygraph examinations. There are legal considerations bearing on the release of polygraph-derived information, all of which are pertinent to possible jeopardy of the polygraph program. Further, I am not authorized at this time to release polygraph information for the stated purpose; release is governed by DCI guidelines which do not provide for dissemination of polygraph-derived information outside of established liaison channels. Finally, the imposition of penalties is directly concerned with the DCI's authority to protect intelligence sources and methods and the ISOO charter (Section 5-2) does not supplant said authority. I do not dispute the need for an independent

oversight authority, but cannot countenance an extension of oversight that might endanger our most effective security tool. It is recommended that the Agency oppose the requirement to report each case of unauthorized disclosure.

6. Other observations:

a. I have no objection to deletion of the section that concerned portion marking.

b. Section 2-201 defines derivative classification as "the determination that information is in substance the same as information currently classified, and the application of the same classification markings." This is confusing and possibly inaccurate in that new information assigned a derivative classification may have a relationship to, but is seldom the same as that on hand, either in content or substance. It is suggested that the passage be replaced by a definition similar to that given in the Directorate of Administration Classification Guide; the latter definition is more lucid and descriptive.

c. Use of the term "shall" as a replacement for "may" in Section 2-201 seems inconsistent with Section 2-203 which permits waivers of the requirement to prepare classification guides.

d. Relating to the above, the ISOO draft would permit the Agency, when setting up a derivative classification system, to limit the classification to the same categories applicable to original classification. Agency use of this option would represent ultimate simplification of the administrative difficulties associated with preparation and use of guides; there would be no need for derivative classification guides. I recommend the option as a logical and viable approach.

e. Section 4-102, in the ISOO draft, is a very general statement presumably intended to simplify the Order. It may be too simplistic in that the section no longer specifies originating agencies may place restrictions on reproduction and establish accountability controls. The Office of Security has an interest in control markings for Sensitive Compartmented Information (SCI) and would prefer the language of the interagency task force be restored. However, SCI markings are covered by DCID and unlikely to be affected by the Order. The cited deletion is of more concern to the DO and NFAC on noncompartmented information that may

not be reproduced or disseminated without approval of the originator. I defer to the DO and NFAC on this matter.

7. In closing, I wish to iterate my concern over the apparent consequences of Section 4-201. At issue is a basic disagreement that figured prominently in the revision of E.O. 12036, i.e., a Department of Defense (DoD) refusal to accept any language that in a worst case interpretation would permit the DCI to impose security standards the Department is unwilling to accept or unable to implement. In my opinion, based on extensive participation in deliberation of the DCI Security Committee, the DoD misgivings are completely unfounded; the collegial approach in spirit and practice precludes any intrusion into areas that represent DoD prerogatives. I contend that the ISOO draft is contrary to the letter of the National Security Act of 1947 and, in this context, unacceptable as a compromise to satisfy DoD concerns. The bottom line, if the Agency accepts surrender or fragmentation of the Director of Central Intelligence's responsibility, is that the title would be meaningless.

STAT [redacted]

Distribution:
Orig - Adse
1 - OS Registry
1 - D/Security
1 - PPG Chrono

STAT OS/P&M/PPG/[redacted]slb (3 November 1981)

0660/8

05 1